misc

- Remy's Epic Adventure

Remy's Epic Adventure

Task

We're given a short platformer and we have to beat it to get the flag.

Solution

So firstly I "beat" the game normally. But the problem is that the final boss' health doesn't even budge when you hit him, but task author ensured that his health is being affected.

So I had to cheat a bit.

First thing I tried was autoclicker. It sure helps with beginning levels, but boss still seems invincible. So then my teammates told me about sth called CheatEngine - simple program to cheating in simple games. Just what we need.
One of the options is game tick acceleration, but even with autoclicker it wasn't enough. So I concluded I had to directly alter the boss' health.
Other useful option in CheatEngine is searching for values. You can search for places in memory that have given property.

So normally one would search for boss' health and modify it. But I didn't know exact value so I came up with another plan. I guessed boss health is four byte integer. So I search for 4-byte integers lower than 0xffffffff. Then a got couple hits in and from previous findings searched for such that value decreased. After about five iterations there was only four possible values and one was decreasing by 1 when I was hitting the boss.

So I changed it to 10 and when I resumed the game boss health bar disappeared. I finished it of and there was the finish. And there I was at the title screen happy about myself. Here comes a guy, pulling the flag out from behind the screen. (will add photos later)

When there was about two thirds of flag visible he stopped. And then he jumped quickly showing the flag for split-second. Eh...

So I had to repeat the process, but I got to the title screen I used CheatEngine speed alteration to slow down the game 10 times and recorded the display with my phone. Then I read the whole flag that is WPI{j0in_th3_illumin@ti_w1th_m3}.